ML:MWG
F.#2019R01370

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF THE ELECTRONIC DEVICES KNOWN AND DESCRIBED AS: (1) ONE CHROME AND SILVER APPLE IPHONE CELLULAR DEVICE, MODEL IPHONE 11 PRO, LABELED "SM" AND "10/09/19" IN BLACK MARKER; AND (2) ONE APPLE IMAC COMPUTER, SERIAL NUMBER C02NGEHKF8J2, EMC NUMBER 2638	APPLICATION FOR A SEARCH WARRANT FOR ELECTRONIC DEVICES Case No. 19-MJ-928

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, STEVEN MULLEN, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property – two electronic devices – which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations ("HSI") and am assigned to the Child Exploitation Investigations Unit. My responsibilities include investigations of cases involving the promotion of a sexual performance by a child through the use of electronic devices and the internet, possession and distribution of child pornography through the use of

electronic devices and the internet, human trafficking and other incidents of the exploitation of children on the internet. I have gained expertise in this area through training in classes and daily work related to conducting these types of investigations. As part of my training and experience, I also have gained expertise in the identification of minor victims. As part of my responsibilities, I have been involved in the investigation of numerous child pornography and child exploitation cases. I am familiar with the facts and circumstances set forth below from my participation in the investigation; my review of the investigative file; and from reports of other law enforcement officers involved in the investigation.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The properties to be searched are (a) one chrome and silver Apple iPhone cellular device, Model iPhone 11 Pro, Labeled "SM" and "10/09/19" in black marker ("DEVICE-1") and (b) one Apple iMac computer, serial number C02NGEHKF8J2, EMC number 2638 ("DEVICE-2"). DEVICE-1 and DEVICE-2 (collectively, the "DEVICES") are currently located in the custody of HSI within the Eastern District of New York.

5. The applied-for warrant would authorize the forensic examination of the DEVICES for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. In June 2019, HSI began investigating VICTOR HUGO GALARZA ("GALARZA") for sex tourism in violation of 18 U.S.C. § 2423. During the course of the

investigation, HSI developed probable cause to believe that GALARZA has produced and possessed child pornography, in violation of 18 U.S.C. §§ 2251, 2252 and 2252A.

7. GALARZA is a United States citizen residing in Queens, New York. GALARZA travels frequently to Colombia through JFK International Airport.

8. On or about June 11, 2019, GALARZA was stopped by law enforcement agents as he entered the United States from Colombia, and his cell phone was detained and its contents searched pursuant to the border search doctrine. The cell phone was subsequently returned to GALARZA the next day after a forensic image of its contents was created.

9. On or about August 13, 2019, GALARZA was again stopped by law enforcement agents as he entered the United States from Colombia, and his cell phone (the same cell phone that was previously detained) and its contents were searched pursuant to the border search doctrine.

10. During the searches of the detained phone, law enforcement recovered four video files depicting another individual (hereinafter "Co-Conspirator-1") engaging in sexual activity with a minor individual (hereinafter "Victim-1"), who, as described below, was sixteen years old at the time. GALARAZA's voice can be heard on the video files directing Co-Conspirator-1 and Victim-1 to engage in specific sexual activity.

11. On or about June 7, 2019, GALARZA exchanged messages via WhatsApp with another individual (hereinafter "Co-Conspirator-2") concerning a time to meet Victim-1. Specifically, on or about June 7, 2019, at approximately 9:09 a.m., GALARZA wrote to Co-Conspirator-2: "[Victim-1] is set. 1 p.m. Miro girls set for 7 p.m." Later that day, at

approximately 11:13 a.m., GALARZA wrote to Co-Conspirator-2: "See you at 1pm. [Victim-1] is set."

12. At approximately 12:35 p.m., GALARZA sent Victim-1 a text message with a certain address in Medellin, Colombia (the "Medellin Location").

13. Metadata for the four above-described video files shows that the video files were created on June 7, 2019, between approximately 3:07 p.m. and approximately 3:20 p.m. at the Medellin Location.

14. Law enforcement agents interviewed Victim-1 on or about September 26, 2019. Victim-1 stated that she is currently sixteen years old.[1] Victim-1 positively identified a photograph of GALARZA as "Victor." Victim-1 explained, in sum and substance and in part, that, on or about June 7, 2019, "Victor" had paid her approximately one million Colombian pesos in cash to have sex with Co-Conspirator-1 while "Victor" remained in the room. After being shown photographs of the Medellin Location, Victim-1 positively identified the Medellin Location as the place where she was paid by "Victor" to have sex with Co-Conspirator-1. Victim-1 also identified herself in a still photograph from one of the video files created on June 7, 2019, that was recovered from GALARZA's cell phone.

15. HSI has reason to believe that GALARZA has produced child pornography and engaged in sex tourism in Colombia on other occasions. In approximately June 2019, an individual (hereinafter "Individual-1") told law enforcement agents that, when she was less

[1] HSI agents have obtained a copy of Victim-1's birth certificate, which confirms that Victim-1 is currently sixteen years old.

than eighteen years old, GALARZA, while in Colombia, paid her in money and narcotics to perform oral sex on him. Individual-1 also stated that GALARZA arranged for her later to have sex with Co-Conspirator-1 and that she was paid with money and narcotics. At some point, GALARZA asked Individual-1 to provide him with other, younger girls for sex. After Individual-1 turned eighteen years old, GALARZA paid Individual-1 and another individual who was seventeen years old at the time (hereinafter "Individual-2") in money and narcotics to have sex with Co-Conspirator-1 and for the sexual encounter to be recorded. That video was recorded on Individual-1's phone, and Individual-1 provided the video to HSI. GALARZA can be seen on the video wearing red shorts with a white stripe and holding up a phone as if it is recording. In approximately June 2019, Individual-2 confirmed that she was seventeen years old at the time of the above-referenced video and that GALARZA had paid her in money and narcotics to make a pornographic video with Individual-1.

16. The searches of GALARZA's phone revealed conversations between GALARZA and Co-Conspirator-2 appearing to discuss sex with underage girls. On June 7, 2019, Galarza sent a photo of a young female to an individual and wrote the following messages:

> 15 yrs old
> Raw dog
> Out of farm system
> For tonight ?

Co-Conspirator-2 responded: "Hell fucking yes" and "You know I want that." GALARZA responded in a voice message, in sum and substance, that this girl had a twin sister. In addition, GALARZA's phones contain a recording of an individual other than GALARZA

having sex with two girls who appear to be twins and, based on my training and experience, appear to be less than eighteen years old.

17. Often, in conversations with Co-Conspirator-2 discussed above, GALARZA and the individual discuss the price of girls in Colombian pesos. In another conversation, an individual said he had oral sex with a girl ("Individual-3") who said she was sixteen years old, and GALARZA responded that the girl was actually fifteen.

18. Several other videos from GALARZA's phone show Co-Conspirator-1 having sex with young girls who appear to be less than eighteen years of age. On the videos, GALARAZA's voice can be heard directing Co-Conspirator-1 and the young girls to engage in specific sexual activity.

19. On October 8, 2019, the Honorable Peggy Kuo, United States Magistrate Judge for the Eastern District of New York, signed an arrest warrant for GALARZA based upon a complaint charging GALARZA with having violated 18 U.S.C. § 2251 (production of child pornography). See 19-MJ-908.

20. HSI agents, including myself, arrested GALARZA the next day at his home in Queens, New York. Thereafter, GALARZA was detained and advised of his Miranda rights. GALARZA waived his Miranda rights and agreed to speak with law enforcement. After waiving his Miranda rights, GALARZA made the following statements, in sum and substance and in part, which were audio recorded by HSI. GALARZA admitted that he had produced approximately thirty to forty pornographic videos of Co-Conspirator-1 engaging in sexual activity with young females in Colombia, that he did so over a period of approximately eight years, that DEVICE-1 (GALARZA's cell phone) contained such videos,

that he transferred such videos to DEVICE-2 (GALARZA's desktop computer) and that he sold electronic copies of such videos to friends in exchange for payments via PayPal. GALARZA further stated that he had most recently sold an electronic copy of a pornographic video, which depicted Co-Conspirator-1 engaging in sexual activity with a young female, the day before his arrest via WhatsApp. GALARZA further stated that he arranged for Co-Conspirator-2, a United States citizen, to have sex with a fifteen year old girl in Colombia.

21. HSI agents asked if GALARZA consented to law enforcement's seizure and search of the DEVICES. After law enforcement agents advised GALARZA of his right not to consent to a search of the DEVICES without a search warrant and informed him that anything found in such a search could be used against him, GALARZA gave written consent to law enforcement to seize and search the DEVICES. After GALARZA gave such consent, I seized the DEVICES and wrote "SM" and "10/09/19" on the back of DEVICE-1 in black marker.

22. The DEVICES are currently in the lawful possession of HSI in the Eastern District of New York. HSI agents seized the DEVICES following GALARZA's statements that he uses the DEVICES to store pornographic videos of Co-Conspirator-1 engaging in sexual activity with other individuals.

23. As described above, GALARZA gave written consent to law enforcement to seize and search the DEVICES. Therefore, while HSI might already have all necessary authority to examine the DEVICES, I seek this additional warrant out of an abundance of

caution to be certain that an examination of the DEVICES will comply with the Fourth Amendment and other applicable laws.

TECHNICAL TERMS

24. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or

locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also

include global positioning system ("GPS") technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static – that is, long-term – IP addresses, while other computers have dynamic – that is, frequently changed – IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

25. Based on my training, experience and research, I know that DEVICE-1 has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. Based on my training, experience and research, I know that DEVICE-2 has capabilities that allow it to serve as a digital camera and media player. In my training and experience, examining data stored on devices of this type can

uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

26. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

27. There is probable cause to believe that things that were once stored on the DEVICES may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the storage medium that is not currently being used by an active file – for long periods of time before they are

overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media – in particular, computers' internal hard drives – contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

28. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the DEVICES were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the DEVICES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word

processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer

behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses an electronic device to sell child pornography over the Internet, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

29. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the DEVICES consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the DEVICES to human inspection in order to determine whether it is evidence described by the warrant.

30. *Manner of execution.* Because this warrant seeks only permission to examine DEVICES already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

31. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the DEVICES described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

STEVEN MULLEN
Special Agent
United States Department of Homeland Security, Homeland Security Investigations

Subscribed and sworn to before me by telephone on October 11, 2019:

THE HONORABLE PEGGY KUO
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

The properties to be searched are (a) one chrome and silver Apple iPhone cellular device, Model iPhone 11 Pro, Labeled "SM" and "10/09/19" in black marker ("DEVICE-1") and (b) one Apple iMac computer, serial number C02NGEHKF8J2, EMC number 2638 ("DEVICE-2"). DEVICE-1 and DEVICE-2 (collectively, the "DEVICES") are currently located in the custody of HSI within the Eastern District of New York.

This warrant authorizes the forensic examination of the DEVICES for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the DEVICES described in Attachment A that relate to violations of 18 U.S.C. §§ 2251, 2252, 2252A, and 2423 and involve VICTOR HUGO GALARZA, Co-Conspirator-1 and Co-Conspirator-2 since January 1, 2011, including:

a. images of child pornography and files containing images of child pornography and records, images, information or correspondence pertaining to the possession, access with intent to view, receipt and distribution of sexually explicit material relating to children, in violation 18 U.S.C. §§ 2252 and 2252A, in any form wherever they may be stored or found;

b. motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

c. records and information pertaining to the preparation, purchase and acquisition of names or lists of names to be used in connection with the purchase, sale, trade or transmission of any visual depiction of minors engaged in sexually explicit conduct;

d. records and information pertaining to the production of any visual depiction of a minor engaged in sexually explicit conduct;

e. records and information pertaining to the distribution of any visual depiction of a minor engaged in sexually explicit conduct;

f. records and information pertaining to the transportation of any visual depiction of a minor engaged in sexually explicit conduct to the United States;

g. records and information concerning any Internet accounts used to possess, receive or distribute child pornography;

h. evidence regarding traveling with intent to engage in illicit sexual conduct and engaging in illicit sexual conduct in foreign places in violation of 18 U.S.C. § 2423, including but not limited to conversations with individuals regarding sex with minors and giving drugs to minors, photographs and videos (whether pornographic or not) regarding minors, and any other information (such as contact lists) on the DEVICES regarding minors.

2. Evidence of user attribution showing who used or owned the DEVICES at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history, including:

a. records of Internet Protocol addresses used;

b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.